FULL VERSION OF PENDING CLAIMS

Claim 1 (Currently Amended): A cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption,

the cipher strength estimating device comprising an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body, wherein:

the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

the session key prospect calculating section is operative to: calculate one session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation;

the untransformed text calculating unit body is operative to: calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed

yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; and repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect.

Claim 2 (Original): A cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption,

the cipher strength estimating device comprising an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body, wherein:

the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

the session key prospect calculating section is operative to: dynamically create a condition for use in calculating one session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate the session key prospect based on the condition thus created or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation;

the untransformed text calculating unit body is operative to: calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the

recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect.

Claim 3 (Currently Amended): A cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption,

the cipher strength estimating device comprising an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body, wherein:

the untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

the session key prospect calculating section is operative to: dynamically create conditions for use in calculating a session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate the session key prospect based on the conditions thus

created or identify inability to calculate when inconsistency is found between certain two of the conditions and then output uncalculability identifier data indicative of inability to calculate; and optionally calculate another session key prospect for the relevant round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation;

the untransformed text calculating unit body is operative to calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the untransformed text calculating unit; receive the putative untransformed text outputted; repeatedly further input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the untransformed text calculating unit together with the plaintext; and optionally output the recalculation request data to the session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the session key prospect calculating section to cause the session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect.

Claim 4 (Currently Amended): A cipher strength estimating device for estimating a strength of a ciphertext which is a transformed text obtained at a final round of a transformation process including: receiving a plaintext; transforming the plaintext using, as a parameter, a session key calculated from a key for use in encryption; and repeatedly further transforming the resulting transformed text which is the plaintext thus transformed to perform stepwise encryption,

the cipher strength estimating device comprising a first untransformed text calculating unit, a second untransformed text calculating unit, and a control unit, the first untransformed text calculating unit comprising an untransformed text calculating unit body and a first session key prospect calculating section, the second untransformed text calculating unit comprising a second session key prospect calculating section, wherein:

the first untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

the second untransformed text calculating unit is operative to receive, as inputs thereto, the plaintext and one of the ciphertext obtained at the final round of the transformation process and a putative transformed text presumed to be a transformed text obtained at a certain intermediate round;

the first session key prospect calculating section is operative to: conduct brute-force search for the session key to be used at a certain round of transformation by using the plaintext and one of the ciphertext and the putative transformed text; calculate one session key prospect

presumed to be equivalent to the session key to be used at said certain round of transformation or output uncalculability identifier data indicative of inability to calculate when the calculation is impossible; and optionally calculate another session key prospect for said certain round which is different from the session key prospect already outputted in response to receipt of recalculation request data requesting recalculation;

the second session key prospect calculating section is operative to: dynamically create plural conditions for use in calculating a session key prospect presumed to be equivalent to the session key to be used at a relevant round of transformation by higher order differential cryptanalysis using the plaintext and one of the ciphertext and the putative transformed text; and calculate one session key prospect based on the conditions thus created or identify inability to calculate when inconsistency is found between certain two of the conditions and then output uncalculability identifier data indicative of inability to calculate;

the untransformed text calculating unit body is operative to calculate a putative untransformed text presumed to be equivalent to an untransformed text which is not transformed yet at the relevant round based on the session key prospect and one of the ciphertext and the putative transformed text; and output the putative untransformed text as an output of the untransformed text calculating unit; and

the control unit is operative to: input the plaintext and one of the ciphertext obtained at the final round of the transformation process and the putative transformed text obtained at the certain intermediate round, which make a pair, to the first untransformed text calculating unit; receive the putative untransformed text outputted; input the putative untransformed text as a putative transformed text for a round immediately preceding the relevant round to the second untransformed text calculating unit together with the plaintext; and optionally output the

recalculation request data to the first session key prospect calculating section in response to receipt of the uncalculability identifier data outputted from the second session key prospect calculating section to cause the first session key prospect calculating section to again calculate said another session key prospect for the immediately preceding round and then output the putative untransformed text based on said another session key prospect.